(19) Japanese Patent Office (JP)
(12) Patent Office Gazette (A)
(11) Laid-Open No. 154989/2001 (Heisei 13)
(P2001-154989A)
(43) Laid-open date: June 8, 2001
(21) Application No. 341289/1999 (Heisei 11)
(22) Application Date: November 30, 1999
(71) Applicant: 000006747
Ricoh Company, Ltd.
3-6, Nakamagome 1-chome, Ota-ku, Tokyo

(72) Inventors: Masuyoshi TANEUCHIDA, Yoichi KANAI, Tomio MIZUNO, Tatsuya FURUKAWA, Yoichi ISHIKAWA
c/o Ricoh Company, Ltd.
3-6, Nakamagome 1-chome, Ota-ku, Tokyo

[Title of the Invention] Electronic Information Disclosure Certifying Method and System, Recording Medium Where Electronic Information Disclosure Certifying Program is Stored

[Detailed Description of the Invention]

[0001]

[Technical Field Pertinent to the Invention]

The present invention relates to a method, a system and a computer program for certifying that specified electronic information has been disclosed on a network and a storage medium storing the computer program therein.

[Prior Art]

A method and a system for certifying that specified electronic information has existed on specified dates and time have been already proposed. Such method and system are described in US. Patent No. 51366647, US. Reexamination Patent No. RE34954, US. Patent No. 5136646, US. Patent No. 5373561 and US. Patent No. 5781629, for example. However, the art described in the above-mentioned US patents do not serve to certify that specified electronic information is disclosed on a network such as internet.

[0003]

[Problem to be Solved by the Invention]

In these years, technical information has been disclosed in internet or the like, such technical information includes information equivalent to technical information published in magazines and books and the transmission rate is incomparably higher than that of conventional publications. Thus, researchers have increasingly used internet and the like to make their findings public earlier. Furthermore, as compared with the conventional publications, the electronic information can be transmitted more easily and at lower costs, and therefore, there is a high probability that more information will be disclosed in internet and the like. However, according to the conventional art, although it is possible to certify that electronic information exists, it is impossible to certify that electronic information is disclosed in internet and the like. In this case, that is, in the case where it is impossible to certify disclosure in internet and the like, others may acquire a patent having the same concept as the disclosed technical information. As described above, the technical information disclosed in internet and the like achieves the substantially same effect as publications and in Japan, a law that proscribes granting a patent to "inventions available to the public via electronic communication lines" has been established. However, since it is difficult to certify when technical information was disclosed in internet and the like and that technical information is not falsified, it cannot be denied that such information is inferior to conventional publications in credibility as evidence. Furthermore, in HTML (Hyper Text Markup Language) and other types of documents used in internet and the like, various object may be embedded in-line. Some objects require plug-in software of browsers and an auxiliary application as well as static image, moving image, sound and Java applet (Java is a trademark owned by Sun Microsystems. The electronic information disclosed in internet and the like is comprised of the HTML or other type of document and an embedded object and transmitted to the public based on the combination. Hyperlink may be provided in the HTML or other type of document so that an object including the other HTML or other type of document can be referred as an external resource. However, the electronic information disclosed in internet and the like is configured on the precondition that the electronic information is read on-line and when the electronic information is locally preserved, the embedded or referred object cannot be often available from the electronic information. Thus, after disclosure on the network, it is impossible to indicate what electronic information was disclosed. Therefore, the present invention intends to provide a method, a system and a computer program for certifying that specified electronic information is disclosed on prescribed conditions on a network such as internet and the online information transmitting state of the specified electronic information, and a storage medium storing the computer program therein.

[0004]

[Means for Solving Problem]

A method for certifying that specified electronic information is disclosed in a specified computer connected to a network in accordance with a first aspect of the present invention comprises a first step of having access to the specified electronic information stored in the specified computer and copying the specified electronic information and an object when the object is contained in the specified electronic information according to a recording request; a second step of changing the specified electronic information from the locally stored specified electronic information when the specified electronic information and the object are locally stored so as to make the object available, and storing the changed specified electronic information together with the copied object in a storage device; a third step of acquiring an electronic information that uniquely specifies and certifies the copied specified electronic information and object, the changed specified electronic information and attribute information on the location of the specified electronic information on the network together with dates and time; and a fourth step of storing the electronic certificate and the attribute information in the storage device in response to the changed specified electronic information. Thus, since the electronic certificate for both the electronic information itself disclosed on the network and the electronic information by which on-line information transmittance state can be reproduced artificially, that is, the above-mentioned "changed specified electronic information" can be acquired, what information among the whole electronic information is substantially disclosed via the network can be certified later. It is possible to further comprise a fifth step of storing the specified electronic information in the storage device. It is also possible to further comprise a sixth step of providing the client with the electronic certificate, the attribute information and the changed electronic information and object, which are stored in the storage device according to a certifying request or the like. Furthermore, it is possible to a seventh step of having access to a second electronic information or a second object referred from the specified electronic information and copying the second electronic information or the second object, configure the above-mentioned second step so as to include a step of changing the specified electronic information from the locally stored specified electronic information when the specified electronic information, the object and the second electronic information or the second object are locally stored so as to make the object, the second electronic information and the second object available, and configure the above-mentioned third step to be a step of acquiring an electronic information that uniquely specifies and certifies the copied specified electronic information and object, the second electronic information or the second object, the changed specified electronic information and attribute information on the location of the specified electronic information on the network together with dates and time. Thus, the object or the like linked from the specified electronic information can be certified. Internet is the most suitable for the above-mentioned network, and in this case, the electronic information is an electronic information described in markup language such as HTML (Hyper Text Markup Language) and XML (eXtensible Markup Language), the information on the location of the specified electronic information on the network is a uniform resource locator and the object contained in the electronic information is a static image, a moving image, sound, applet or data in a format designated by the electronic information.

[0005]

A method for certifying that specified electronic information is disclosed in a specified computer connected to a network in accordance with a second aspect of the present invention comprises a first step of having access to the specified electronic information stored in the specified computer and copying a second electronic information or object when the specified electronic information refers to the second electronic information or object according to a recording request; a second step of changing the specified electronic information from the locally stored specified electronic information when the specified electronic information and the second electronic information or object are locally stored so as to make the second electronic information or object available, and storing the changed specified electronic information together with the second electronic information or object in a storage device; a third step of acquiring an electronic information that uniquely specifies and certifies the copied specified electronic information and second electronic information or object, the changed specified electronic information and attribute information on the location of the specified electronic information on the network together with dates and time; and a fourth step of the electronic certificate and the attribute information in the storage device in response to the changed specified electronic information. Thus, relationship between the electronic information and the linked second electronic information or object can be reproduced later. A system for certifying that specified electronic information is disclosed in a specified computer connected to a network in accordance with a third aspect of the present invention comprises an access means for having access to the specified electronic information stored in the specified computer and copying the specified electronic information and an object contained in the specified electronic information according to a recording request; a changing means for changing the specified electronic information from the locally stored specified electronic information when the specified electronic information and the object are locally stored so as to make the object available, and storing the changed specified electronic information together with the copied object in a storage device; an electronic certificate acquisition means for acquiring an electronic information that uniquely specifies and certifies the copied specified electronic information and object, the changed specified electronic information and attribute information on the location of the specified electronic information on the network together with dates and time and storing the electronic certificate and the attribute information in the storage device in response to the changed specified electronic information; and a means for providing the electronic certificate and attribute information stored in the storage device, the changed electronic information and the object to the client. In the third aspect of the present invention, the configuration further comprising a means of issuing the electronic information is possible. Modification of the first aspect of the present invention described above can be applied to the system for certifying electronic information disclosure in accordance with the third aspect.

[0006]

A system for certifying electronic information disclosure in accordance with a fourth aspect a means having access to the specified electronic information stored in the specified computer and copying the specified electronic information and second electronic information and object when the specified electronic information refers the second electronic information and object according to a recording request; a means for changing the specified electronic information from the locally stored specified electronic information when the specified electronic information and the second electronic information or object are locally stored so as to make the second electronic information or object available, and storing the changed specified electronic information together with the copied second electronic information or object in a storage device; a means for acquiring an electronic information that uniquely specifies and certifies the copied specified electronic information and second electronic information or object, the changed specified electronic information and attribute information on the location of the specified electronic information on the network together with dates and time and storing the electronic certificate and the attribute information in the storage device in response to the changed specified electronic information; and a means for providing the electronic certificate and attribute information stored in the storage device, the changed electronic information and the second electronic information or object to the client. Further, the methods for certifying electronic information disclosure in accordance with the first and second aspects are each installed as a program for performing in the computer and this program is stored in a storage medium or storage device such as floppy disk, CD-ROM, magnetic optical disk, semiconductor memory and hard disk.

[0007]

[Embodiments]

Firstly, offered services relating to a precondition of the present invention will be described schematically. For example, a client A requests a provider B of this service to (1) record that a web page stored in a WWW (World Wide Web) server of his/her own which is connected to internet is disclosed in internet for a certain period and (2) put a link to the web page so that the public can know the existence and the location of the web page. The service provider B receiving the request has access to the web page of designated URL from an IP address unknown to the client A at any timing unknown to the client A and copies the web page. Next, the service provider B generates attribute information including the URL of the web page, the IP (Internet Protocol) address of an accessor and acquires an electronic certificate that uniquely specifies and certifies the copy and attribute information of the web page together with dates and time. Then, the service provider B associates the copy and attribute information of the web page with the acquired electronic certificate and stores them. The service provider B has access to the web page of designated URL at any timing unknown to the client A again and copies the web page. At this time, by having access to the web page from a changed IP address of the accessor, it is also possible to certify that the WWW server of the client A does not control access. Next, as described above, the service provider B generates attribute information and acquires an electronic certificate that uniquely specifies and certifies the copy and attribute information of the web page together with dates and time. Then, the service provider B associates the copy and attribute information of the web page with the acquired electronic certificate and store them. The service provider B repeats such processing for a certain period designated by the client A. Furthermore, in response to the request (2), the client A places a link to the URL of the designated web page in a web page stored in a WWW (World Wide Web) server of his/her own which is connected to internet so that the public can gain access. For example, the link may be searched by client or contents field. The placement of the link in the WWW server together with placing period is recorded.

[0008]

The client A can request the service provider B to provide contents of recording with respect to the web page designated in the above (1) concurrently with the above-mentioned request or as the need arises. In response to the request, the service provider B provides the copy and attribute information of the stored web page and the electronic certificate. At this time, it is possible to provide the above-mentioned data written into a recording medium such as CD-R or via internet. Further, in response to the above-mentioned request (2), the service provider B may provide the record that link to the designated web page is put in the WWW server of the service provider B and the recording period as the electronic certificate. The client A can use the information provided from the service provider B to certify that the web page is disclosed in internet for a certain period. In addition the above-mentioned (1) and (2), the client A (3) can request the service provider B to record that the designated web page can be searched by a search engine for the public in internet. This certifies that the public can easily know existence and the location of the web page. The service provider B perform search by the search engine by using a suitable keyword and the like. When the designated web page can be searched, the fact that the web page can be searched, an address and name of the used search engine and search date are recorded. This record may be provided as a certificate to the client A according to the request to provide the record.

[0009]

The client A requests the service provider B to record the web page stored in the WWW server of his/her own in (1) and further can request (1)' to record the web page stored in another person's WWW server. In this case, the service provider B performs the operation as described in the above (1). However, there is no guarantee that the web page in the another person's WWW server continues to exist the period designated by the client A and the web page may be deleted or be changed. When the web page is deleted, the service provider B may record the period during which the web page is disclosed in internet and according to the client's request to provide the record, provide the period in addition to the information provided normally. When the web page is changed, history of change is recorded by performing the above-mentioned processing. To record the web page stored in the another person's WWW server, the client A may designate the URL of the web page or all URLs obtained by performing keyword search in the designated search engine. The client A can (4) request the service provider B to record transition of version of the web page stored in the his/her own or another person's WWW server. The service provider B performs the same processing as (1), for example. However, the service provider B inspects whether or not the contents of the web page accessed last time are different from those of the web page accessed this time. When the contents are different from each other, the fact is recorded. The service provider B does not need to store the copied web page. For example, the client A may store the copy. When the service provider B does not store the copied web page, only the attribute information and electronic certificate are stored at each access in the operations (1) and (1)'. In the case of (4), when the contents of the web page accessed last time are different from those of the web page accessed this time, change in version can be stored by storing the difference or whole of the web page. The client A can designate recording period, times, frequency, etc. in the recording requests of (1) and (1)'. According to this, the service provider B performs recording. The services (2) to (4) can be optional, and especially, the services (2) and (3) are unnecessary if existence and the location of the web page are apparent to the public through the other medium and the like.

[0010]

On the other hand, when this service is continued, the service provider B holds a lot of web pages with the electronic certificates for certifying that the web pages are disclosed in internet. Using the information, the service provider B can (5) offer the service of providing web pages with the electronic certificates. For example, the service provider B constructs a database capable of performing keyword search and the like via internet to offer search service to a third person. According to the searcher's request to provide contents of record, the service provider B provide the contents of record via internet of by a recording medium such as CD-R. Alternatively, the service provider B may prepare summaries of web pages with the electronic certificates and construct a database so as to perform screening search by using the summaries. Fig. 1 shows the outline of an electronic information disclosure certification system for providing the services described above. A server A denoted by 3, a server B denoted by 5, a server C denoted by 7, a server D denoted by 9, a server E denoted by 11 and a lot of computers not shown are connected to a network 1. The network 1 is internet, for example. The server A denoted by 3 is a WWW server that stores electronic information such as a web page 31 with an URL of http://www.abcd.co.jp and discloses the page therein. The server B denoted by 5 is a server managed by the service provider that includes a copy acquisition function 51 for having access to electronic information designated by the client and acquiring the copy, an attribute information generation function 53 for generating attribute information containing information of electronic information such as URL and access conditions, a certificate acquisition function 55 for acquiring an electronic certificate that uniquely specifies and certifies the copied electronic information and the attribute information together with dates and time, a storage function 57 for storing necessary information and a certificate provision function for providing the stored electronic certificate in response to the client's request. The server B denoted by 5 is connected to a storage device 61 and the server C denoted by 7 has a time stamp certificate issuance function for issuing the certificate that uniquely specifies and certifies the specified electronic information together with dates and time. The server C denoted by 7 receives a request to issue the certificate via the network 1 and send back the electronic certificate to the client.

[0011]

The server D denoted by 9 is a server for adding a function to the server B denoted by 5 and puts a link 91 to the web page designated by the client as the WWW server. However, a database of the link 91 may be constructed so as to be searchable for each content or owner of the linked web page. Further, there may be cases where a database 95 is constructed by using data in the storage device 61 connected to the server B denoted by 5 and the server D denoted by 9 has a retrieval function 93 for searching the database 95 via the network. Furthermore, there may be cases where summary of each electronic information is prepared from the data in the storage device 61 and the retrieval function 93 can search a database 96 on the summary via the network. The server E denoted by 11 is a search engine for the public. Since the search engine for the public is the same as the conventional search engine, the description thereof is omitted. Next, the services (1) and (1)' offered according to the present invention will be described as the operation of the system shown in Fig. 1. The client A designates the electronic information to be recorded for a certain period as a web page of URL, http://www.abcd.co.jp of the server A denoted by 3 and requests the service provider B to offer the service (1) or (1)'. The service provider B performs processing by using the server B denoted by 5. The copy acquisition function 51 of the server B denoted by 5 has access to http://www.bcd.co.jp through a route (A), for example, at any timing and acquires a copied web page 31 through a route (B). The copy is held in, for example, a main memory of the server B denoted by 5. At each access, the copy acquisition function 51 stores an IP address of the accessor in the storage device. The copy acquisition function 51 includes a function of determining access conditions and determines, for example, that the client make an access at which timing and by using which IP address of the acceccor for a certain period designated by the client. When the client designates frequency, access is scheduled so as to meet the designation of frequency. The attribute information generation function 53 generates attribute information containing the IP address of the accessor and the URL designated by the client A. For example, when the server 5 denoted by 5 is connected to the network 1 through a proxy server not shown, the attribute information may contain an IP address of the proxy server and access dates in addition to the IP address and URL.

[0012]

The certificate acquisition function 55 acquires an electronic certificate for a copy the acquired web page 31 and the generated attribute information. More specific processing will be described in detail later. In the system of Fig. 1, the certificate 55 receives a request to issue the electronic certificate sent through a route (C) in the network 1, for example in the time stamp certificate issuance function 71 of the server C denoted by 7 and receives the electronic certificate issued by the time stamp certificate issuance function 71 through a route (D) in the network 1, for example. The time stamp certificate issuance function 71 will be described in detail later. The storage function 57 stores the copied the web page 31 acquired by the copy acquisition function 51, the attribute information generated by the attribute information generation function 53 and the electronic information acquired by the certificate acquisition function 55 in the storage device 61. However, it is optional that the copy acquisition function 51 stores the copied web page 31 acquired by the copy acquisition function 51. For example, the client A may store the copy by himself/herself. When contents of the web page 31 copied last time are the same as those of the web page 31 accessed this time, the storage function 57 may determine that the copied web page 31 acquired this time is not stored. The storage function 57 stores data for each client or designated URL so that the certificate provision function 59 can pick up necessary data later. The client A requests provision of the record contents concurrently with the recording request or at any timing. At this time, in response to the request, the certificate provision function 59 read out the copied web page 31 as a target of request, the attribute information and the electronic certificate from the storage device 61, stores a recording medium such as a CD-R 63 in the example of Fig. 1 and provides client A with them. Although the copied web page 31, the attribute information and the electronic certificate are stored at each access, the certificate provision function 59 may store all of them in the recording medium such as a CD-R for provision or when the copied web page 31 remains unchanged, may provide the copied web page 31, all attribute information and all electronic certificates at the time of first access. In the certificate provision function 59, it is possible to prepare access record including the URL, IP address of the accessor and dates of certificate by using the attribute information and the electronic certificate and to provide the access record and the copied web page 31, all attribute information and all electronic certificates at the time of first access as the certificate by the service provider B. When the storage function 57 does not store the copied web page

31, the certificate provision function 59 does not provide the client A with the copied web page 31.

[0013]

Next, the service (2) offered according to the present invention will be described on the basis of the system shown in Fig. 1. The service (2) is offered to agree to the client A's request the service provider B to put a link to the web page so that the public can know existence and the location of the web page. In response to the request, the service provider B puts a link 91 to the web page 31 stored in the server A denoted by 3 in the server D denoted by 9, which is connected to the network 1. When the number of requests is small, an URL of the designated web page should be only placed in the web page stored in the server D denoted by 9. When the number of requests is large, there may be cases where a database on the link is constructed and the third person can perform search according to contents of the web page or type of business of the client via the network 1. The service provider B records the period during which the link 91 to the web page 31 is put in his/her own web page and the searchable period in the storage device, and provides the record as the certificate at the request of the client A. Next, the service (3) offered according to the present invention will be described on the basis of the system shown in Fig. 1. The service (3) is offered to agree to request the service provider B to record that the designated web page can be searched in the server E denoted by 11 as a search engine for the public on the network 1. The service provider B makes search in the search engine in the server E denoted by 11 by using a suitable keyword or the like, for example, via the server B denoted by 5, and when the designated web page 31 can be searched, records the fact that the web page can be searched, a name and an address of the server E denoted by 11, the used keyword, search dates and time, etc. When the client A make requests later, this record is provided as the certificate.

[0014]

Next, the service (4) offered according to the present invention will be described on the basis of the system shown in Fig. 1. The service (4) is offered to agree to request the service provider B to record transition of the version of the web page 31. The service provider B performs the same processing as (1) by using the server B denoted by 5. That is, the service provider B has access to the web page 31 of the server A denoted by 3 at a predetermined timing and acquires the copied web page 31. Next, the attribute information containing URL and access conditions is generated and the electronic certificate with respect to the attribute information and the copied web page 31 is acquired. At least attribute information and electronic certificate are stored in the storage device 61. It is also possible to store the copied web page 31 in the storage device 61. Next, an access is made to the web page 31 of the server A denoted by 3 at the predetermined timing, the same processing is performed and the electronic certificate with respect to the attribute information and the web page 31 is acquired. Subsequently, it is determined whether or not contents of the web page 31 accessed last time, more accurately, the web page 31, change of which is detected most recently, are different from those of the web page 31 accessed this time. This determination may be performed by either the copy acquisition function 51 or the storage function 57. When the contents are different from each other, the difference in addition to at least attribute information and electronic certificate are recorded in the storage device. In some cases, the difference between the contents of the web page 31 accessed last time and those of the web page 31 accessed this time may be recorded in the storage device. The copy of whole web page 31 is ensured to be stored in the storage device when the contents are different from each other. At the request of the client A, the service provider B provides at least attribute information, the electronic certificate and the record on presence or absence of change. The whole of web page may be provided each time when the contents are changed.

[0015]

Next, the service offered according to the present invention will be described on the basis of the system shown in Fig. 1. The service (5) is a service of offering the web page with the electronic certificate. The service provider B provides the retrieval function 93 in the server D denoted by 9 and uses the copied web page 31 with the electronic certificate and the attribute information stored in the storage device 61 to construct the data base 95. The service provider B allows the third person to search the database 95 by using the retrieval function 93. When the third person finds the copied web page 31 that he/she intends to use, the third person submits a request to provide the record contents to the service provider B via the network 1 or the like. The service provider B stores the copied web page 31, the attribute information and the electronic certificate in the CD-R 63 or the like by using the certificate provision function 59 and provides the CD-R 63 or the like. The above-mentioned data may be transmitted via the network 1. The service provider B prepares summary from the copied web page 31 and constructs the database 97 of the summary so that the third person can make search by using the retrieval function 93. After screening of the database of the summary, the third person can identify the copied web page 31 and make a request to provide record contents of the necessary electronic information. A processing flow of the main services (1) and (1)' according to the present invention is shown in Fig. 2. When the client A make a recording request with designated recording conditions on electronic information to be recorded such as web page, for example, information on the location of URL and recording period, to the service provider B (step S1), the copy acquisition function 51 determines access conditions (step S3) so as to fulfill the recording conditions, has access to the URL from the predetermined IP address of the accessor and acquires the copied web page (step S5). The attribute information generation function 53 generates attribute information including the URL of the web page and the IP address of the accessor as an access condition (step S7). Subsequently, the certificate acquisition function 55 acquires the electronic certificate that uniquely specifies and certifies attribute information and the copied web page together with dates and time from the time stamp certificate issuance function 71 (step S9). The server B denoted by 5 can be configured so as to contain the time stamp certificate issuance function 71, and in this case, the certificate acquisition function 55 is replaced with the time stamp certificate issuance function 71. The storage function 57 stores at least attribute information and electronic certificate in the storage device 61 (step S11). As described above, it is optional that the copied web page is stored in the storage device. This processing is repeated until the condition for end of recording is fulfilled (step S13). The condition for end of recording is, for example, the case where recording period designated by the client A has finished or the number of recording designated by the client A has reached.

[0016]

Fig. 3 shows a flow of processing performed according to the client A's request to provide record contents. Since the request to provide record contents (step S41) includes electronic information to be recorded, firstly, the certificate provision function 59 identifies electronic information to be recorded (step S43). Then, the certificate provision function 59 reads out the copied electronic information, electronic certificate and attribute information from the storage device 61 (step S45). When recording is requested with one recording request or target electronic information disappears after one access, only one set of data is read out. However, since data is generally recorded multiple times, multiple sets of copied electronic information, attribute information and electronic certificates are read out. The certificate provision function 59 calculates disclosure period additionally (step S47). Since the electronic certificate contains record of dates and time, at least start and end of closure is found by referring the electronic certificate acquired at the first access and the electronic certificate acquired at the last access and this information is defined as disclosure period. However, this processing is optional. Lastly, the certificate provision function 59 stores the copied target electronic information, electronic certificate, attribute information and disclosure period information in a medium such as CD-R, provides the medium (step S49) and the finishes the processing (step S51). Here, the electric certificate will be briefly described with reference to Fig. 4. According to the present invention, so long as the electronic certificate that uniquely specifies and certifies electronic information together with dates and time is issued, the electronic certificate may be issued in any method. Providing that an electronic information 101 is a target of the electronic certificate, firstly, a hash value 103 with respect to the electronic information 101 is calculated. Any one-way function may be used as hash function. For example, the certificate acquisition function 55 calculates the hash value. A request to issue a certificate containing the hash value 103 is sent to the time stamp certificate issuance function 71. The time stamp certificate issuance function 71 performs processing of the hash value together with other hash values sent in the same manner. As shown in Fig. 4, for example, the processing of generating another hash value from two hash values is repeated and a hash value 106 is generated from all of the sent hash values finally. By using the hash value 106 and an SHV (Super Hash Value) 105 at a time T – 1 (T is an integral number), an SHV 107 at a time T is generated. The SHV 107 thus generated, the hash value 103, time information of the time T and a document ID constitute an electronic certificate 109. The electronic certificate 109 is sent to a sender of the hash value 103 and paired with the electronic information 101 to uniquely specify and certify the electronic information 101 together with dates and time.

[0017]

When the web page is regarded as the electronic information in Fig. 4, an HTML document corresponds to the electronic information. However, although there is no problem when the web page contains only text, an image file such as GIF file is generally embedded in the web page. As shown in Fig. 5, for example, when the web page 31 of the server A denoted by 3 is viewed from a browser of a client computer not shown, which is connected to the network 1, a web page 200 in which objects 201 and 203 such as static images are in-line embedded is represented. A moving image, sound, a file in the format requiring plug-in of the browser and Java applet (trademark owned by Sun Microsystems) may be embedded in the web page. In such case, contents of the object embedded in the web page is included in the information disclosed on the network. In Fig. 5, for example, links 205 to 209 to the other web pages or objects as external resources are included in the web page 200. Although the web pages or objects at places to be linked cannot be regarded as the contents disclosed in the URL of the web page, the user of the network 1 can easily obtain electronic information at the places to be linked. Thus, the electronic information has an availability for the public. Further, the web pages or objects linked to the link 205 to 209 have often relevance to the web page 200 and the creator of the HTML document of the web page 200 may intend to disclose the information that is combined the web page 200 and the linked web pages or objects. Thus, the problem that the web pages or objects at places to be linked are made subject for electronic certificates occurs. In addition, the HTML document and the objects 201 and 203 of the web page 200 shown in Fig. 5, for example, respectively, are locally stored as a file in the server 5 shown in Fig. 5, for example, and the locally stored HTML document is viewed by the browser. As shown in Fig. 6, only frames 201a and 203a of the above-mentioned objects 201 and 203 are displayed in a web page 200a. In some cases, marks 201b and 203b indicating these objects are not loaded are displayed within frames. Even when the links 205 to 209 are selected by a pointer, the linked web pages or objects cannot be viewed.

[0018]

This is due to that there are the following HTML descriptions in the HTML document of the web page 200. Table 1 shows the case where the object is in-line embedded. Table 2 shows the case where an external source is used by using a link.

[Table 1]

```
<IMG SRC="image/image01.gif">
<OBJECT DATA="/video/video.avi"TYPE="video/avi"></OBJECT>
<APPLET                         CODE="/applet/animator.class"WIDTH=100
HEIGHT=100></APPLET>
```

[Table 2]

```
<A HREF="/image/image02.gif">1. Image</A>
<A HREF="http://www.xyza.co.jp/home.html>2. Web page</A>
```

First line of Table 1 means that a directory named as image exists under a directory in which the HTML document of the web page 200 exists and a GIF file image01.gif in the image directory is displayed. As a matter of course, when the HTML document of the web page 200 is stored in the server B denoted by 5, there is no guarantee that the directory named as image exists under the directory in which the HTML document is stored and the GIF file image01.gif is stored in the image directory. Second line of Table 1 means that a directory named as video exists under a directory in which the HTML document of the web page 200 exists and a moving image file video/avi video.avi is displayed in MIME format in the video directory is displayed. As a matter of course, when the HTML document of the web page 200 is stored in the server B denoted by 5, there is no guarantee that the directory named as video exists under the directory in which the HTML document is stored and the video avi is stored in the video directory. Third line of Table 1 means that a directory named as applet exists under a directory in which the HTML document of the web page 200 exists, Java applet animator. class in the applet directory is executed and predetermined display is made within a frame 100 X 100. Like the above-mentioned cases, when the HTML document of the web page 200 is stored in the server B denoted by 5, there is no guarantee that the directory named as applet exists under a directory in which the HTML document is stored and applet.class is stored in the applet directory.

[0019]

First line of Table 2 means that a directory named as image exists under a directory in which the HTML document of the web page 200 exists and a link is put to a GIF file image01.gif in the image directory. Since the link is merely put and contents of the file is not displayed when the HTML document is displayed, the contents of the file is not automatically sent via the network 1. Even when the HTML document of the web page 200 is locally stored in the server B denoted by 5, there is no guarantee that the directory named as image exists under the directory in which the HTML document is stored and the GIF file image01.gif is stored in the image directory. Second line of Table 2 means that a link is put to a web page of URL: http://www.xyz.co.jp/home.html which is distinct from the server in which the HTML document of the web page 200 is stored. Since the link is merely put and contents of the file is not displayed when the HTML document of the web page 200 is displayed, the HTML document of the linked web page is not automatically sent via the network 1. Even when the HTML document of the web page 200 is locally stored in the server B denoted by 5, the storage place is not the URL: http://www.xyz.co.jp/home.html. As described above, in the case where the HTML document of the web page 200 is locally stored in the server B denoted by 5, for example, even when the user tries to confirm the contents by using the browser, in-line embedded objects or contents at the places to be linked cannot be viewed. Thus, even when the HTML document is stored, contents disclosed on the network 1 cannot be accurately grasped later. Therefore, according to the present invention, one copy of the HTML document of the web page 200 is stored as an original as it is and another copy is changed so that the contents of the whole web page can be grasped when viewed later. For example, in the cases of Table 1 and Table 2, the HTML document of the web page 200 is changed as follows.

[Table 3]

```
<IMG SRC="image01.gif">
<OBJECT DATA="video.avi"TYPE="video/avi2></OBJECT>
<APPLET CODE="animator.class"WIDTH=100><APPLET>
```

[Table 4]

```
<A HREF="/reference/image02.gif">1. Image</A?
<A HREF="/reference/home.html>2. Web page</A>
```

[0020]

Table 3 means that an in-line embedded object is stored in the same directory as the changed HTML document. It is due to that storing the attribute information, electronic certificate, HTML document of the web page 200 and changed HTML document together with the object in the same directory is convenient in terms of management. However, it is merely an example and as a rule for storing data in the storage device 61 connected to the server B denoted by 5, it is possible to prepare a distinct directory for storing the in-line embedded object therein and store the data in the directory.

Table 4 means that an object or a HTML document of other web page, which is referred as an external resource, is stored in a directory named as reference that exists under the directory in which the changed HTML document is stored. Since the object or the HTML document of the other web page referred as an external resource may not be acquired, a directory is prepared separately and the data is stored in the directory. However, it is merely an example and as a rule for storing data in the storage device 61 connected to the server B denoted by 5, it is possible to store the object or the HTML document of the other web page referred as an external resource together with the original HTML document and the changed HTML document in the same directory. In the case where the web page contains the in-line embedded object and the object or the other web page is referred as an external resource, the file of the HTML document of the web page as an original and the object or HTML document which is in-line embedded or referred as an external resource are stored as they are and the changed HTML document is generated and stored for reference. Then, the electronic certificate with respect to these files and attribute information is acquired. Thus, the configuration of the server B denoted by 5 in Fig. 1 is modified to the configuration of a server 5' in Fig. 7. That is, a copy acquisition function 151 acquires the in-line embedded object and the object or the other web page referred as an external resource in addition to the designated electronic information. A copy modification function 153 changes sources of the in-line embedded object and the referred object or other web page, as described above. An attribute information generation function 155 generates attribute information on these electronic information and objects. At this time, when copies of the referred electronic information and object are acquired, the original reference source may be contained in the attribute information. Information on what types of copied file is targeted for issuance of the electronic certificate may be also contained. A certificate acquisition function 157 acquires the electronic certificate for the information to which the certificate should be issued from the certificate issuance function 71. A storage function 159 stores the file targeted for issuance of the electronic certificate in a storage device 61'. The storage device 61' stores the copied electronic information, modified copy, electronic certificate and object (here, the in-line embedded object) therein. According to the request to provide the record contents, a certificate provision function 161 reads out the information stored in the storage device 61' and prepare a

CD-R 63', for example. Since the modified copy and object are contained in the CD-R 63', the same state as the state where the electronic information targeted for certification is disclosed on online can be reproduced. It can be determined optionally whether the copied electronic information prior to modification is stored or provided according to the request to provide the record contents.

[0021]

Next, a procedure performed according to the recording request will be described with reference to Fig. 8. When the client A makes the recording request that designates information (for example, URL) on the location of the electronic information to be recorded (for example, web page) and recording conditions (for example, recording period) to the service provider B (step S61), the copy acquisition function 151 determines access conditions so as to fulfill the recording conditions (step S63), has access to the URL from the IP address of the predetermined accessor at a predetermined timing and acquires the copied web page (step S65). The copy acquisition processing will be described in detail later. The recording request may include an instruction to copy the designated URL and the link contained in the URL of the web page up to three lower hierarchies. According to the instruction, the copy acquisition 151 copies the linked web page or object. Next, the copy modification function 153 determines whether or not the copied web page contains the object or link (step S67). In the case where the copy modification function 153 contains either object or link, for example, as described above, when the link represented in the copied web page is selected so that the in-line embedded object is displayed on the copy of the locally-stored web page, the copy modification function 153 modifies the copied HTML document of the web page so that contents of the linked web page or object are displayed (step S69). On the other hand, when the copied web page does not contain the link or object, the operation proceeds to the step S71. The attribute information generation function 155 generates the attribute information containing the URL of the web page and the IP address of the accessor as an access condition (step S71). Next, when the copied web page, attribute information and in-line object or link exist, the electronic certificate with respect to the copy of the HTML document of the modified web page, the copy of the in-line embedded object and the copy of the HTML document or object referred as an external resource is acquired from the time stamp certificate issuance function 71 (step

S73). The storage function 159 stores all of information that is uniquely specified and certified together with dates and time by the electronic certificate in the storage device 61' (step S75). It is optional that the copied HTML document of the web page is stored in the storage device. This processing is repeated until the conditions for end of recording is fulfilled (step S77). The condition for end of recording is, for example, the case where recording period designated by the client A has finished or the number of recording designated by the client A has reached.

[0022]

The processing of copy acquisition described with reference to Fig. 8 will be described in more detail by using Fig. 9. Firstly, a copy of the HTML document of the accessed web page designated by the client A is acquired (step S93). This copy of the HTML document of the accessed web page designated by the client is analyzed and it is inspected whether or not the in-line embedded object is included in the copy (step S95). When the object is included, a copy of the object is also acquired (step S97). If the object is not included, the operation proceeds to a step S99. Next, it is determined whether or not a link to the web page or object exists (step S99). When the link exists, a copy of the HTML document or object of the accessed web page is acquired (step S101). If the link does not exist, the processing is finished. In Fig. 9, the copy of the web page or object of the accessed designated web page up to a lower hierarchy is acquired. However, when the copy of the web page or object up to further lower hierarchy is acquired, the web page to be referred is regarded as the designated place to be accessed in the step S93 and the processing in Fig. 9 is performed. At this time, when the place to be linked below a certain hierarchy is not target for copy acquisition, the processing only should be finished without performing the steps S99 and S101. The electronic certificate with respect to the acquired and generated information is acquired in this manner. However, when the electronic certificate as shown in Fig. 4 is acquired, the following mode is possible to calculate the hash value to be generated firstly. As shown in Fig. 10, when the object is in-line embedded and no external resource is referred, it is considered to generate one hash value by combining the file of the HTML document of the accessed web page, the file of the object (in some cases, plural objects exist. Two objects of the object 1 and the object 2 are shown in Fig. 10), the file of attribute information and the file of the changed HTML document. Further, as shown in Fig. 11, when the object is in-line embedded and the external resource is referred to, it is considered to generate one hash value by combining the file of the HTML document of the accessed web page, the file of the object, the file of attribute information, the file of the changed HTML document and the file of the HTML document or object of the referred web page. Whereby, one electronic certificate is acquired. Further, as shown in Fig. 12, when the object is in-line embedded and the external resource is referred, it is considered to generate a first hash value by combining the file of the HTML document of the accessed web page, the file of the object, the file of attribute information and the file of the changed HTML document and to generate a second hash value with respect to the file of the HTML document or object of the referred web page and the attribute information on the HTML document of the referred web page. Since a separate electronic certificate for the HTML document of the referred web page is issued in this manner, it becomes possible to certify that the document is separately disclosed on the network. Concerning the web page referred as the external resource, a lower hierarchy may exist as a reference source and this is handled according to the client's A instruction. When the client A gives no instruction, a general rule that one lower hierarchy is acquired may apply. When the object is in-line embedded also in the referred web page, the object may be handled as being contained in the referred web page.

[0023]

Fig. 13 shows the processing according to the request to provide the record contents. The certificate provision function 161 specifies electronic information to be certified according to the client's A request to provide the record contents (step S81). The copy of target electronic information, the electronic certificate, the attribute information, the in-line embedded object, the referred object or electronic information and the modified copy of the target electronic information are read out from the storage device 61' and provided with being stored in the CD-R 63' or the like (step S85). In response to the request to provide the record contents in the above-mentioned service (5), the processing in Fig. 13 is performed similarly. The operation described above is merely an example and various modification is possible. For example, although the six functions are contained in one server B denoted by 5' in Fig. 7, the functions may be distributed to multiple servers. Similarly, although the link to the requested web page is placed and the retrieval function is provided in the server D denoted by 9, they may be performed in different servers. The number of the search engine for the public is not limited to one and the engine can address ftp as well as http. Furthermore, it is possible to include the function of the server C denoted by 7 in the server B denoted by 5. A subject performing the service by the server C denoted by 7 and a subject performing the service by the server B denoted by 5' may be the same as or different from each other. The network 1 is not limited to internet and can be extended to a network that allows the other nonexclusive access and a network on which the user is treated nonexclusively. Although a CD-R is used as a medium for providing the record contents, this is merely an example and the other medium such as CD-ROM and DVD can be used. The separation of the function blocks is merely an example and it is possible separate one function block into plural function blocks or to combine the plural function blocks into one function block. Based on the combination of the program a computer for fulfilling functions of the function blocks shown in Fig. 1 and Fig. 7, it is possible to configure the devices shown in Fig. 1 and Fig. 7 or to realize a part or whole by using a dedicated electronic circuit, etc.

[0024]

[Effect of the Invention]

The present invention can provide a method, system and computer program for certifying that specified electronic information is disclosed on prescribed conditions on a network such as internet and the online information transmitting state of the specified electronic information and a storage medium storing the computer program therein.

[Brief Description of Drawings]

[Fig. 1] A block diagram of the outline of a system according to the present invention.

[Fig. 2] A flow chart showing an example of processing performed according to a request to record electronic information.

[Fig. 3] A flow chart showing an example of processing performed according to a request to provide record contents.

[Fig. 4] A schematic view showing an example of processing of issuing an electronic certificate that uniquely specifies and certifies electronic information together with dates and time.

[Fig. 5] An example of a display screen in the case where a web page is viewed off-line.

[Fig. 6] An example of a display screen in the case where a web page is viewed off-line.

[Fig. 7] A function block diagram in the case where a server B (5) in Fig. 1 is changed to a server B (5').

[Fig. 9] A flow chart showing an example of processing performed according to a request to record electronic information.

[Fig. 10] A schematic view showing an example of calculation of a hash value.

[Fig. 11] A schematic view showing an example of calculation of a hash value.

[Fig. 12] A schematic view showing an example of calculation of a hash value.

[Fig. 13] A flow chart showing an example of processing performed according to a request to provide record contents.

[Description of Reference Numerals]

1: Network
3: Server A
5: Server B   5': Server B
7: Server C
9: Server D
11: Server E
31: Web page
51: Copy acquisition function
53: Attribute information generation function
55: Certificate acquisition function
57: Storage function
59: Certificate provision function
61: Storage function   61': Storage function
63: CD-R   63': CD-R
71: Time stamp certificate issuance function
91: Link
93: Retrieval function
97: Abstract database
151: Copy acquisition function
153: Copy modification function
157: Certificate acquisition function

159: Storage function

161: Certificate provision function

Claims

1. A method for certifying that specified electronic information is disclosed in a specified computer connected to a network comprising:

a first step of having access to the specified electronic information stored in the specified computer and copying the specified electronic information and an object when the object is contained in the specified electronic information according to a recording request;

a second step of changing the specified electronic information from the locally stored specified electronic information when the specified electronic information and the object are locally stored so as to make the object available, and storing the changed specified electronic information together with the copied object in a storage device;

a third step of acquiring electronic information that uniquely specifies and certifies the copied specified electronic information and object, the changed specified electronic information and attribute information on the location of the specified electronic information on the network together with dates and time; and

a fourth step of storing the electronic certificate and the attribute information in the storage device in response to the changed specified electronic information.

2. An method for certifying electronic information disclosure as stated in claim 1 further comprising a fifth step of storing the copied specified electronic information in the storage device.

3. An method for certifying electronic information disclosure as stated in claim 1 further comprising a sixth step of providing the client with the electronic certificate, the attribute information and the changed electronic information and object, which are stored in the storage device.

4. An method for certifying electronic information disclosure as stated in claim 1 further comprising a seventh step of having access to a second electronic information or a second object referred from the specified electronic information and copying the second electronic information or the second object, wherein

the second step includes

a step of changing the specified electronic information from the locally stored specified electronic information when the specified electronic information, the object and the second electronic information or the second object are locally stored so as to make the object, the second electronic information and the second object available, and

the third step is

a step of acquiring electronic information that uniquely specifies and certifies the copied specified electronic information and object, the second electronic information or the second object, the changed specified electronic information and attribute information on the location of the specified electronic information on the network together with dates and time.

5. An method for certifying electronic information disclosure as stated in claim 1, wherein

the network is internet,

the electronic information is a document described in mark-up language,

the information on the location of the specified electronic information on the network is a uniform resource locator and

the object contained in the electronic information is a static image, a moving image, sound, applet or data in a format designated by the electronic information.

6. A method for certifying that specified electronic information is disclosed in a specified computer connected to a network comprising:

a first step of having access to the specified electronic information stored in the specified computer and copying a second electronic information or object when the specified electronic information refers to the second electronic information or object according to a recording request;

a second step of changing the specified electronic information from the locally stored specified electronic information when the specified electronic information and the second electronic information or object are locally stored so as to make the second electronic information or object available, and storing the changed specified electronic information together with the second electronic information or object in a storage device;

a third step of acquiring electronic information that uniquely specifies and certifies the copied specified electronic information and second electronic information or object, the changed specified electronic information and attribute information on the location of the specified electronic information on the network together with dates and time; and

a fourth step of the electronic certificate and the attribute information in the storage device in response to the changed specified electronic information.

7. A system for certifying that specified electronic information is disclosed in a specified computer connected to a network comprising:

an access means for having access to the specified electronic information stored in the specified computer and copying the specified electronic information and an object contained in the specified electronic information according to a recording request;

a changing means for changing the specified electronic information from the locally stored specified electronic information when the specified electronic information and the object are locally stored so as to make the object available, and storing the changed specified electronic information together with the copied object in a storage device;

an electronic certificate acquisition means for acquiring an electronic information that uniquely specifies and certifies the copied specified electronic information and object, the changed specified electronic information and attribute information on the location of the specified electronic information on the network together with dates and time and storing the electronic certificate and the attribute information in the storage device in response to the changed specified electronic information; and

a means for providing the electronic certificate and attribute information stored in the storage device, the changed electronic information and the object to the client.

8. A system for certifying electronic information disclosure as stated in claim 7, wherein the access means stores the copied specified electronic information in the storage device.

9. A system for certifying electronic information disclosure as stated in claim 7 further comprising a means for issuing the electronic certificate.

10. A system for certifying electronic information disclosure as stated in claim 7, wherein

the access means has access to a second electronic information or a second object referred from the specified electronic information and copies the second electronic information or the second object,

the changing means changes the specified electronic information from the locally stored specified electronic information when the specified electronic information, the object and the second electronic information or the second object are locally stored so as to make the object, the second electronic information and the second object available, and

the electronic certification means acquires an electronic information that uniquely specifies and certifies the copied specified electronic information and object, the second electronic information or the second object, the changed specified electronic information and attribute information on the location of the specified electronic information on the network together with dates and time.

11. An system for certifying electronic information disclosure as stated in claim 7, wherein

the network is internet,

the electronic information is a document described in mark-up language,

the information on the location of the specified electronic information on the network is a uniform resource locator and

the object contained in the electronic information is a static image, a moving image, sound, applet or data in a format designated by the electronic information.

12. A system for certifying that specified electronic information is disclosed in a specified computer connected to a network comprising:

a means having access to the specified electronic information stored in the specified computer and copying the specified electronic information and second electronic information and object when the specified electronic information refers the second electronic information and object according to a recording request;

a means for changing the specified electronic information from the locally stored specified electronic information when the specified electronic information and the second electronic information or object are locally stored so as to make the second electronic information or object available, and storing the changed specified electronic information together with the copied second electronic information or object in a storage device;

a means for acquiring an electronic information that uniquely specifies and certifies the copied specified electronic information and second electronic information or object, the changed specified electronic information and attribute information on the location of the specified electronic information on the network together with dates and time and storing the electronic certificate and the attribute information in the storage device in response to the changed specified electronic information; and

a means for providing the electronic certificate and attribute information stored in the storage device, the changed electronic information and the second electronic information or object to the client.

13. A storage medium that stores a program for certifying that specified electronic information is disclosed in a specified computer connected to a network, wherein

the program for performing

a first step of having access to the specified electronic information stored in the specified computer and copying the specified electronic information and an object contained in the specified electronic information according to a recording request,

a second step of changing the specified electronic information from the locally stored specified electronic information when the specified electronic information and the object are locally stored so as to make the object available, and storing the changed specified electronic information together with the copied object in a storage device,

a third step of acquiring an electronic information that uniquely specifies and certifies the copied specified electronic information and object, the changed specified electronic information and attribute information on the location of the specified electronic information on the network together with dates and time, and

a fourth step of storing the electronic certificate and the attribute information in the storage device in response to the changed specified electronic information,

is stored in a computer other than the specified computer.

14. A storage medium that stores a program for certifying that specified electronic information is disclosed in a specified computer connected to a network, wherein

the program for performing

a first step of having access to the specified electronic information stored in the specified computer and copying the specified electronic information and a second electronic information or object when the specified electronic information refers the second electronic information or object according to a recording request,

a second step of changing the specified electronic information from the locally stored specified electronic information when the specified electronic information and the second electronic information or object are locally stored so as to make the second electronic information or object available, and storing the changed specified electronic information together with the copied second electronic information or object in a storage device,

a third step of acquiring an electronic information that uniquely specifies and certifies the copied specified electronic information and second electronic information or object, the changed specified electronic information and attribute information on the location of the specified electronic information on the network together with dates and time, and

a fourth step of storing the electronic certificate and the attribute information in the storage device in response to the changed specified electronic information,

is stored in a computer other than the specified computer.

[Abstract]

[Problem]

To certify that specified electronic information is disclosed on prescribed conditions on a network such as internet and the online information transmitting state of the specified electronic information.

[Solving Means]

According to a recording request, specified electronic information stored in a specified computer is accessed and the specified electronic information and an object, which is contained in the relevant specified electronic information, are copied. Next, when the specified electronic information and the object are locally preserved, the specified electronic information is changed so that the object can be utilized from the locally preserved specified electronic information, and the changed specified electronic information is stored in a storage device together with the copied object. An electronic certificate, which uniquely specifies and certifies the copied specified electronic information and object, the changed specified electronic information and attribute information with contained information on the location of the specified electronic information together with dates and time, is acquired. With this electronic certificate or the like, the disclosure and the information transmitting state can be certified.

FIG. 1

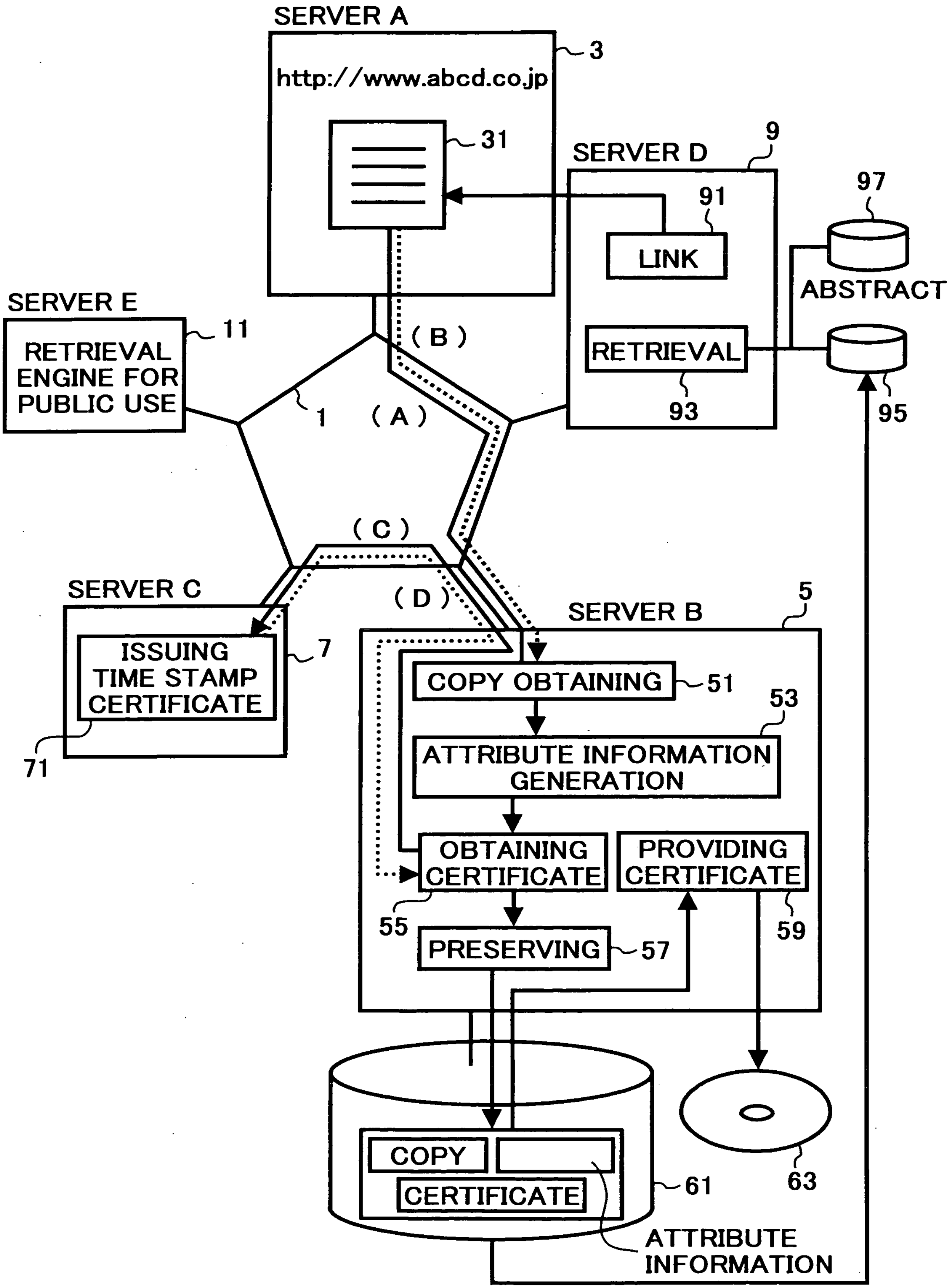

SERVER A
3
http://www.abcd.co.jp
31
SERVER D
9
97
91
LINK
ABSTRACT
SERVER E
11
RETRIEVAL ENGINE FOR PUBLIC USE
(B)
RETRIEVAL
1
(A)
93
95
(C)
SERVER C
(D)
5
SERVER B
ISSUING TIME STAMP CERTIFICATE
7
COPY OBTAINING
51
53
71
ATTRIBUTE INFORMATION GENERATION
OBTAINING CERTIFICATE
PROVIDING CERTIFICATE
55
59
PRESERVING
57
COPY
CERTIFICATE
61
63
ATTRIBUTE INFORMATION

FIG. 2

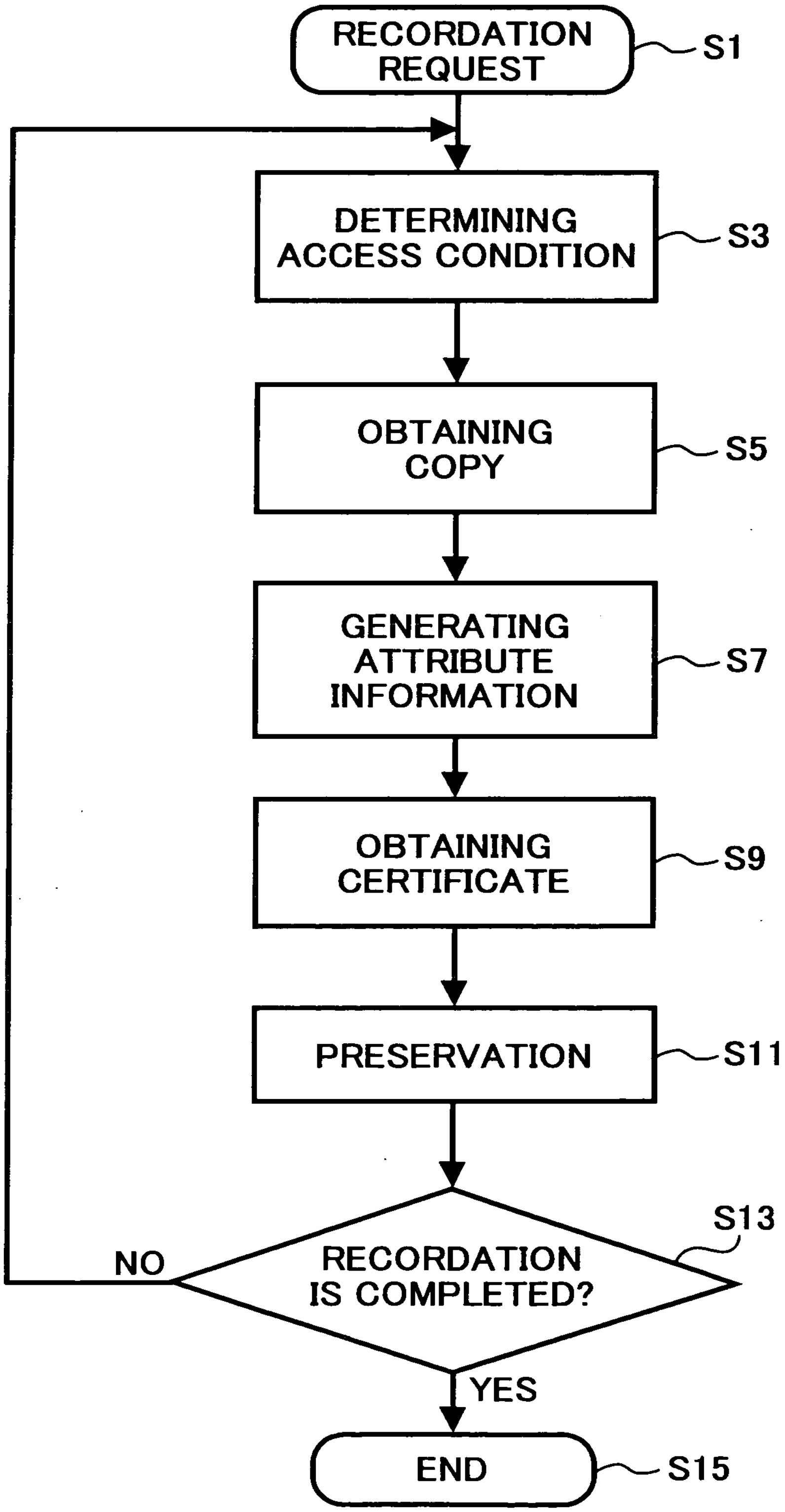

RECORDATION REQUEST
S1
DETERMINING ACCESS CONDITION
S3
OBTAINING COPY
S5
GENERATING ATTRIBUTE INFORMATION
S7
OBTAINING CERTIFICATE
S9
PRESERVATION
S11
S13
NO
RECORDATION IS COMPLETED?
YES
END
S15

FIG. 3

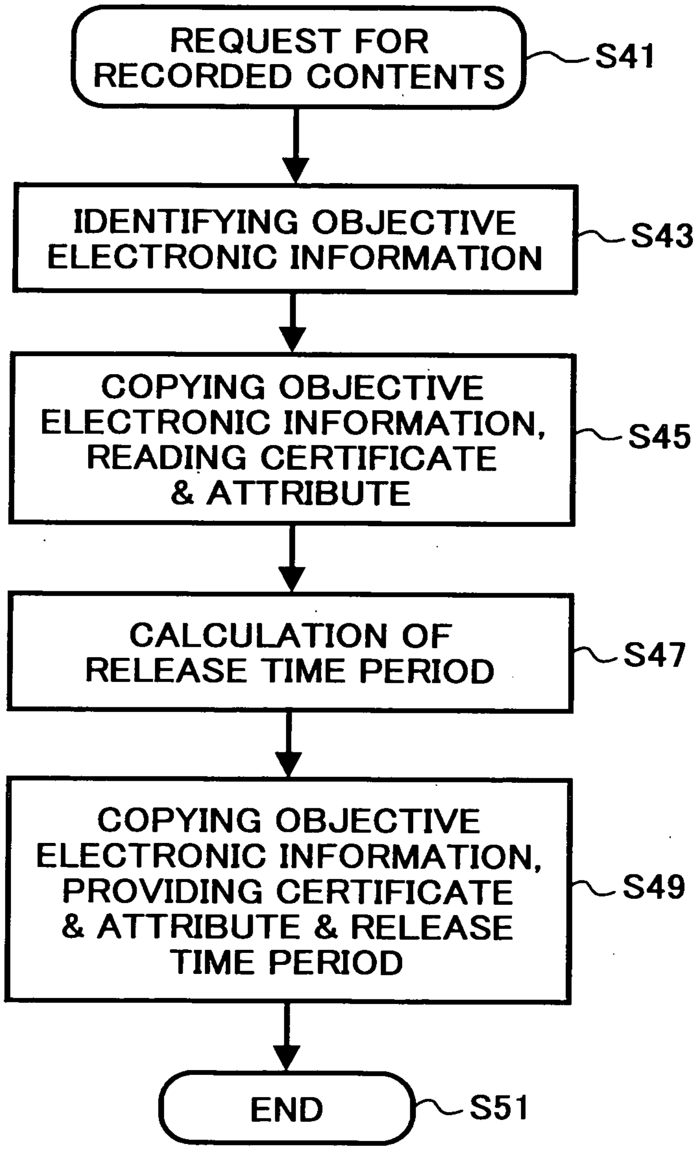

REQUEST FOR RECORDED CONTENTS
S41
IDENTIFYING OBJECTIVE ELECTRONIC INFORMATION
S43
COPYING OBJECTIVE ELECTRONIC INFORMATION, READING CERTIFICATE & ATTRIBUTE
S45
CALCULATION OF RELEASE TIME PERIOD
S47
COPYING OBJECTIVE ELECTRONIC INFORMATION, PROVIDING CERTIFICATE & ATTRIBUTE & RELEASE TIME PERIOD
S49
END
S51

FIG. 4

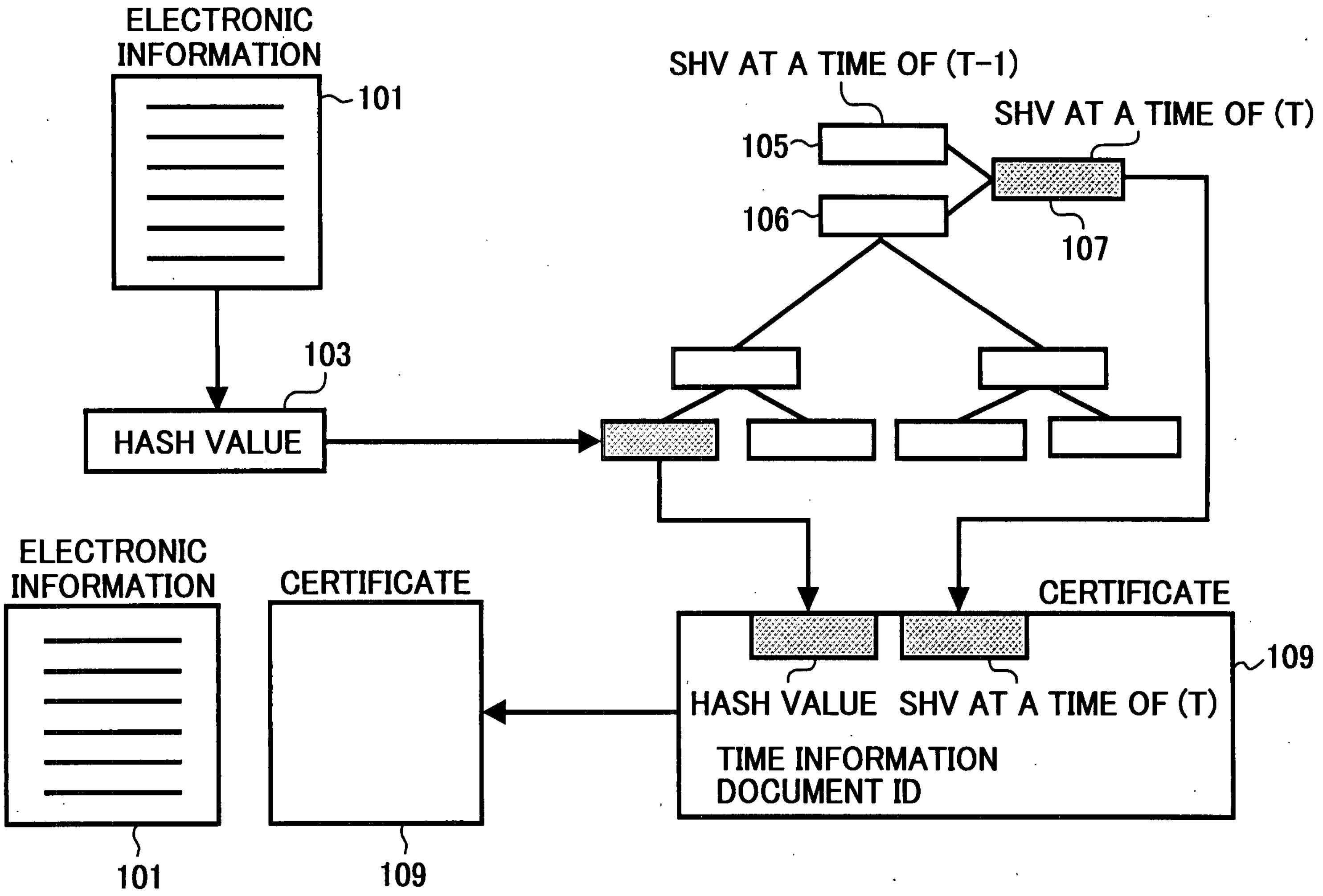

ELECTRONIC INFORMATION
101
103
HASH VALUE
SHV AT A TIME OF (T−1)
105
106
SHV AT A TIME OF (T)
107
CERTIFICATE
109
HASH VALUE
SHV AT A TIME OF (T)
TIME INFORMATION
DOCUMENT ID
ELECTRONIC INFORMATION
CERTIFICATE
101
109

FIG. 5

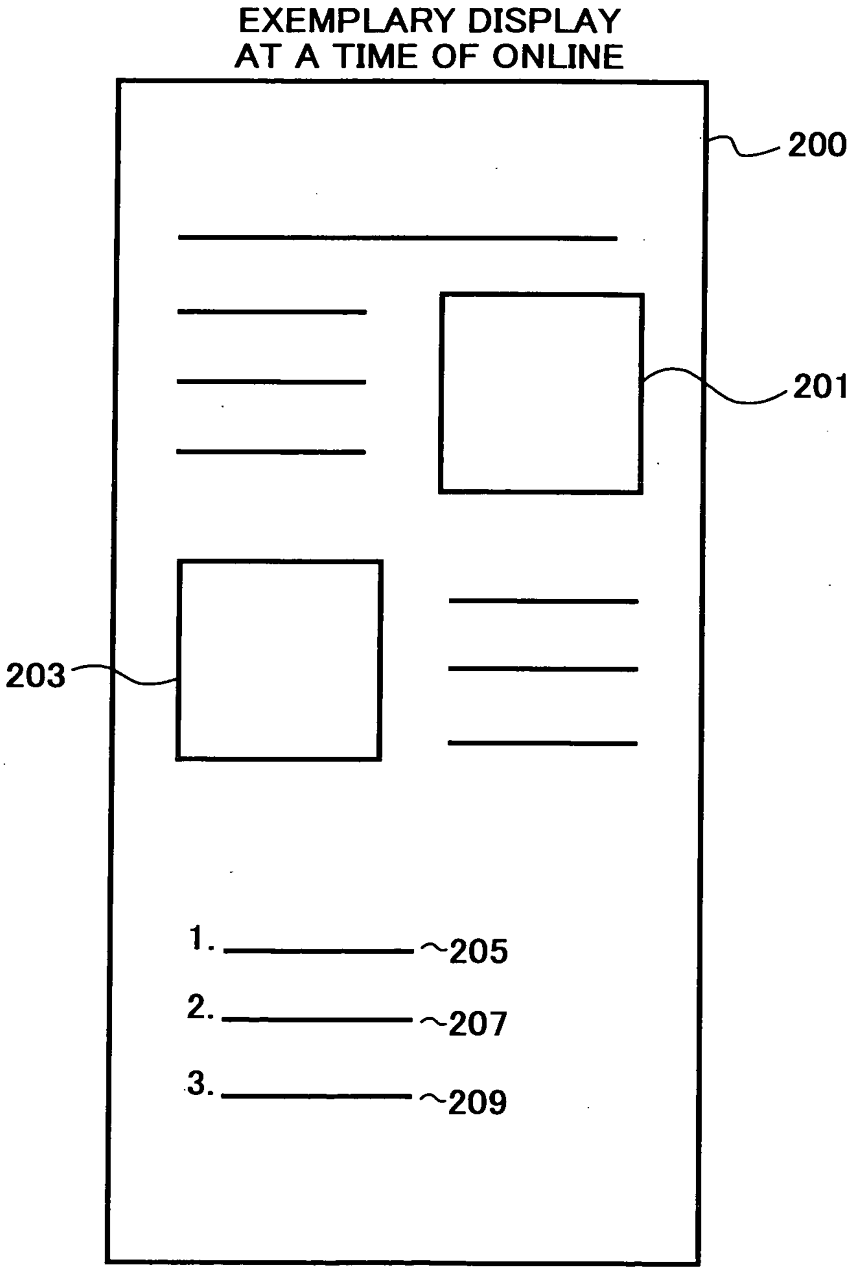

EXEMPLARY DISPLAY
AT A TIME OF ONLINE
200
201
203
1.
205
2.
207
3.
209

FIG. 6

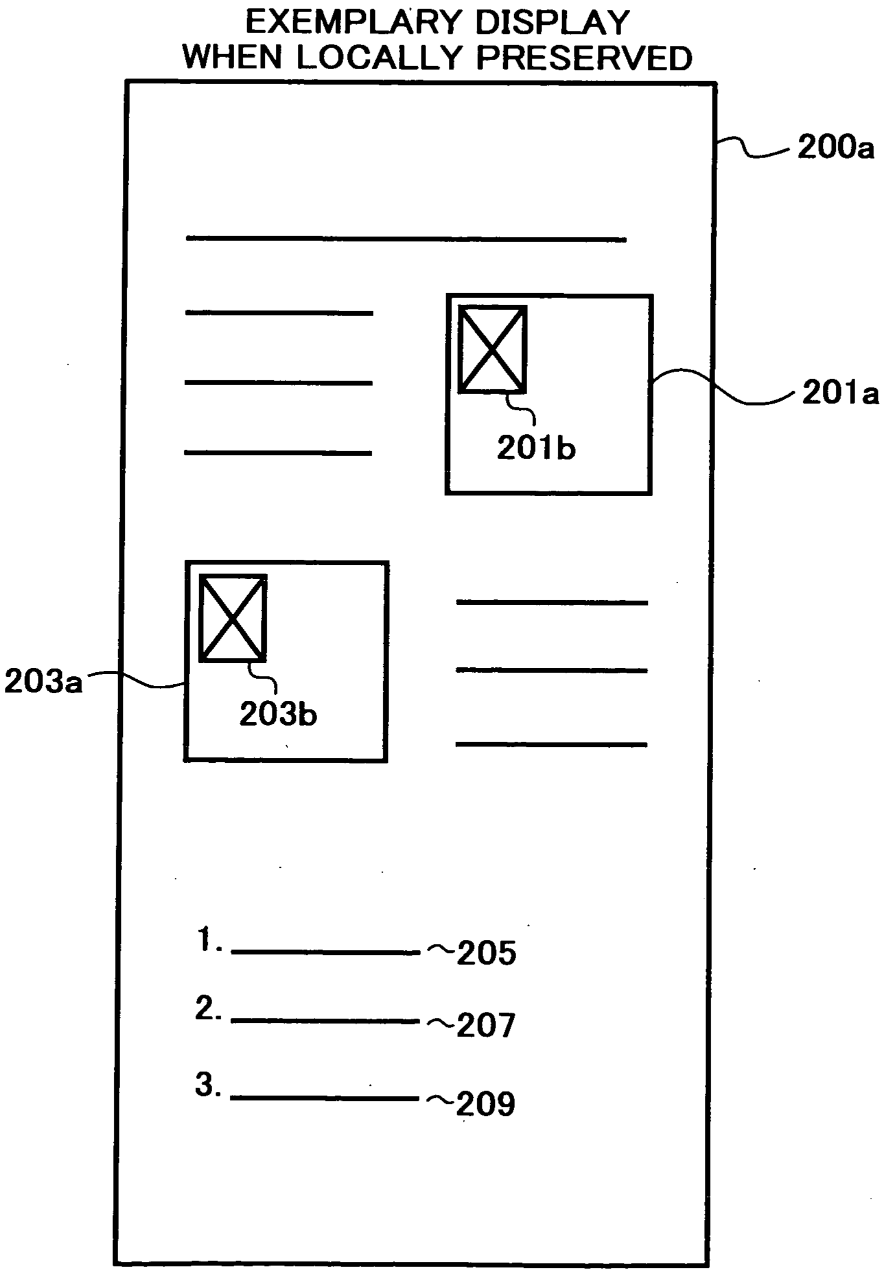

EXEMPLARY DISPLAY
WHEN LOCALLY PRESERVED
200a
201a
201b
203a
203b
1.
205
2.
207
3.
209

FIG. 7

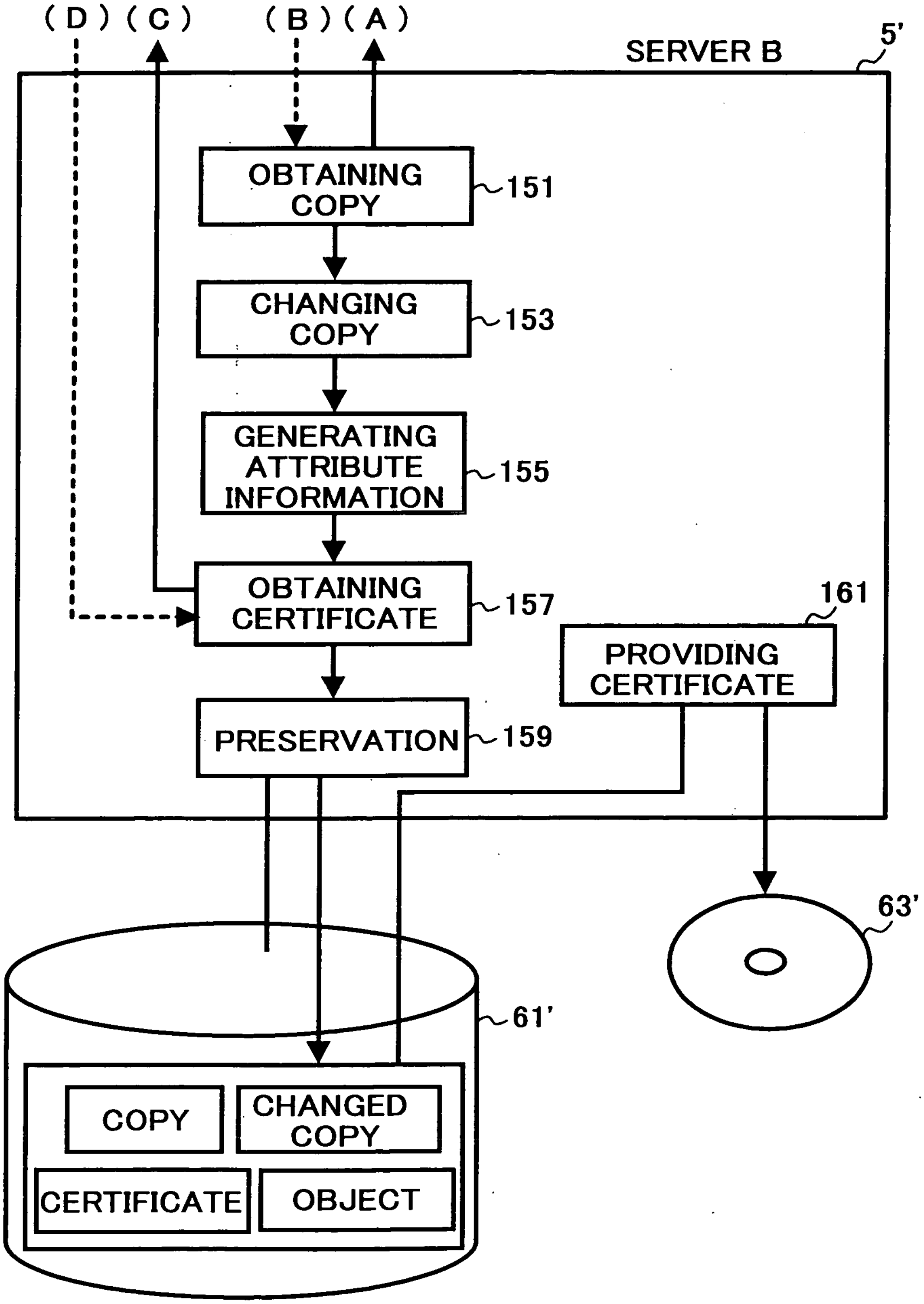

(D)
(C)
(B)
(A)
SERVER B
5'
OBTAINING COPY
151
CHANGING COPY
153
GENERATING ATTRIBUTE INFORMATION
155
OBTAINING CERTIFICATE
157
161
PROVIDING CERTIFICATE
PRESERVATION
159
63'
61'
COPY
CHANGED COPY
CERTIFICATE
OBJECT

FIG. 8

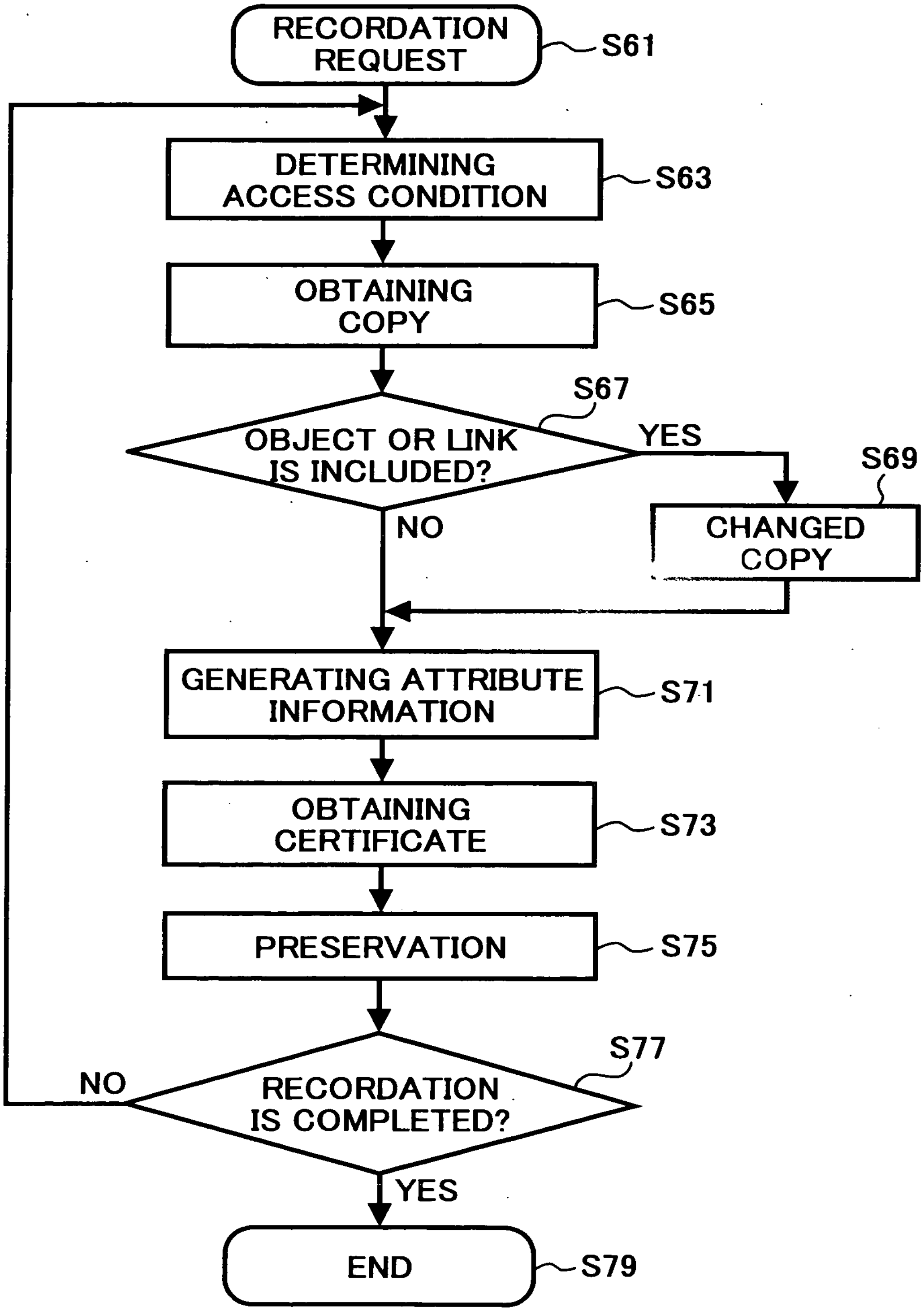

RECORDATION REQUEST
S61
DETERMINING ACCESS CONDITION
S63
OBTAINING COPY
S65
S67
OBJECT OR LINK IS INCLUDED?
YES
S69
CHANGED COPY
NO
GENERATING ATTRIBUTE INFORMATION
S71
OBTAINING CERTIFICATE
S73
PRESERVATION
S75
S77
NO
RECORDATION IS COMPLETED?
YES
END
S79

FIG. 9

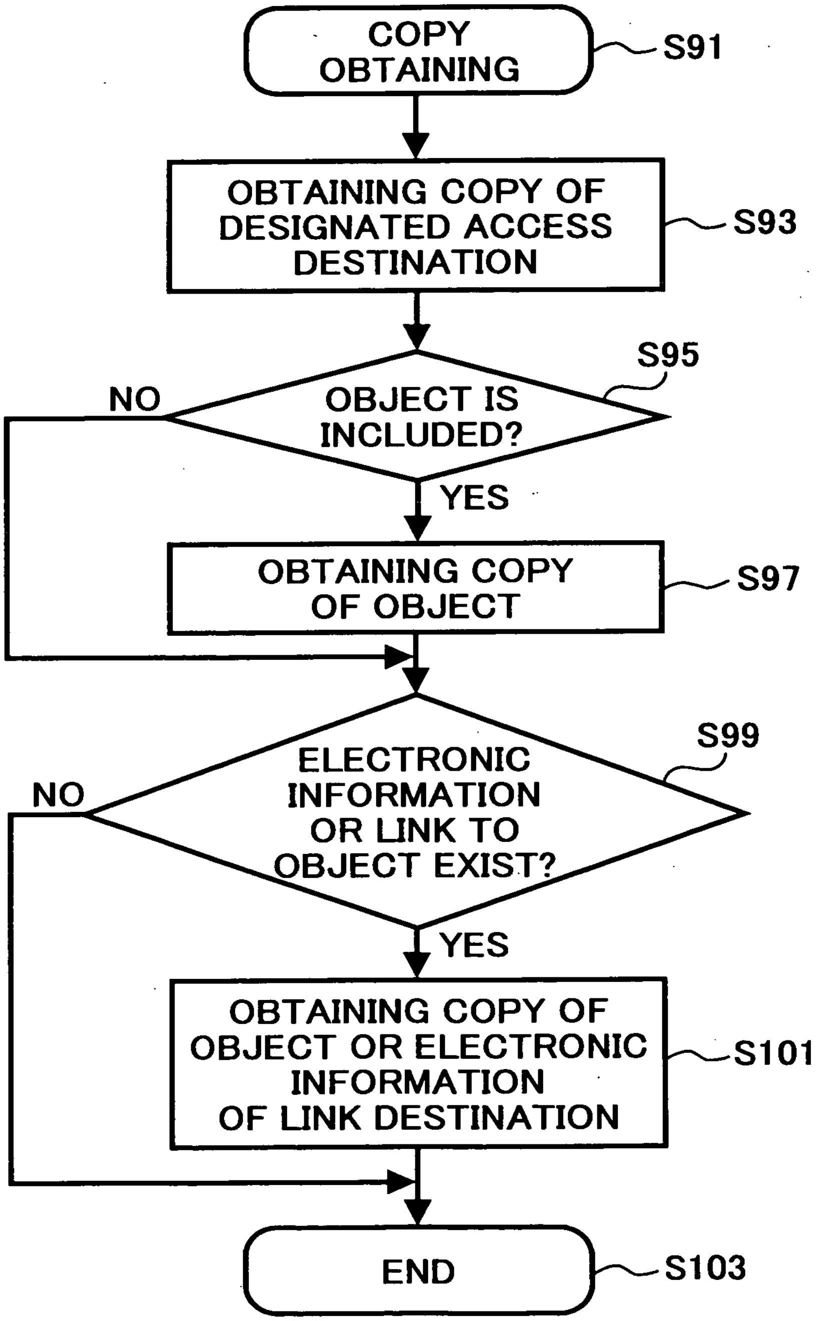

COPY OBTAINING
S91
OBTAINING COPY OF DESIGNATED ACCESS DESTINATION
S93
S95
NO
OBJECT IS INCLUDED?
YES
OBTAINING COPY OF OBJECT
S97
S99
NO
ELECTRONIC INFORMATION OR LINK TO OBJECT EXIST?
YES
OBTAINING COPY OF OBJECT OR ELECTRONIC INFORMATION OF LINK DESTINATION
S101
END
S103

FIG. 10

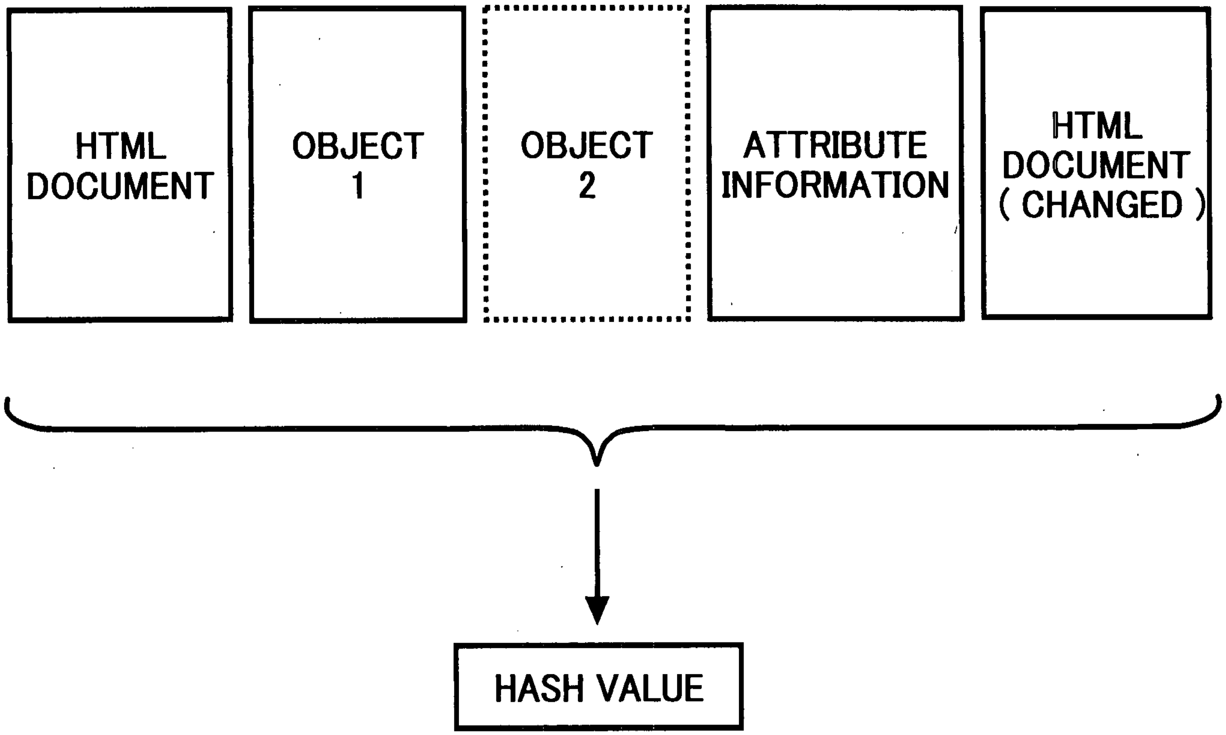

HTML DOCUMENT
OBJECT 1
OBJECT 2
ATTRIBUTE INFORMATION
HTML DOCUMENT (CHANGED)
HASH VALUE

FIG. 11

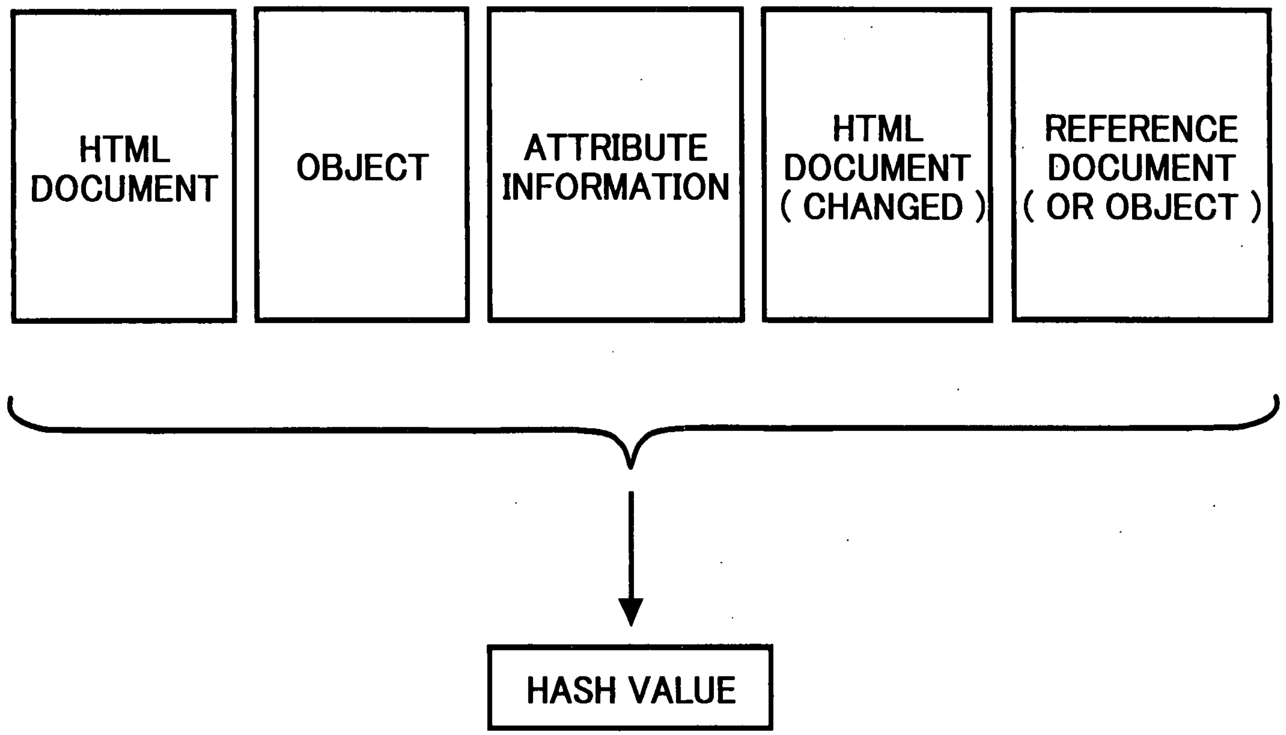

HTML DOCUMENT
OBJECT
ATTRIBUTE INFORMATION
HTML DOCUMENT (CHANGED)
REFERENCE DOCUMENT (OR OBJECT)
HASH VALUE

FIG. 12

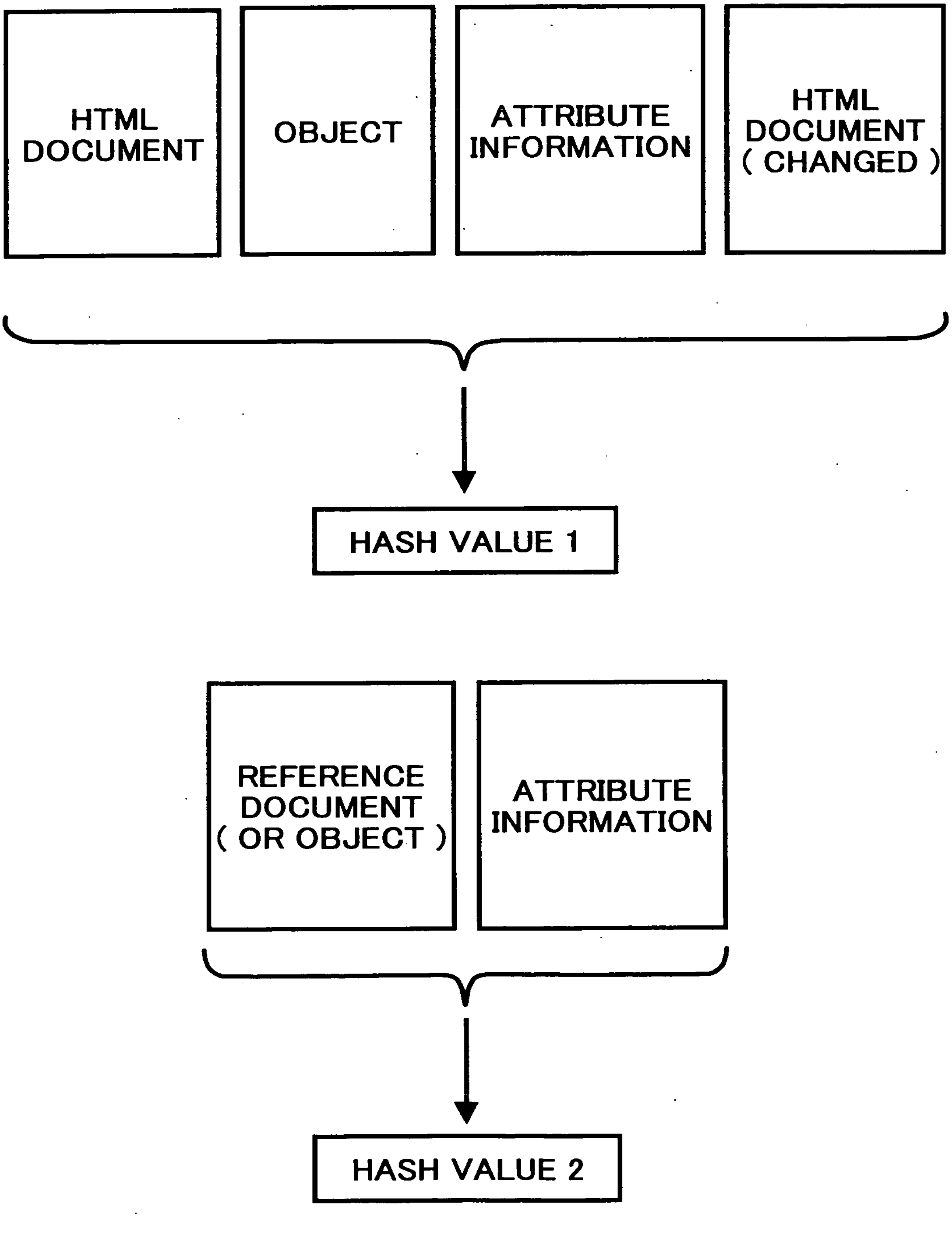
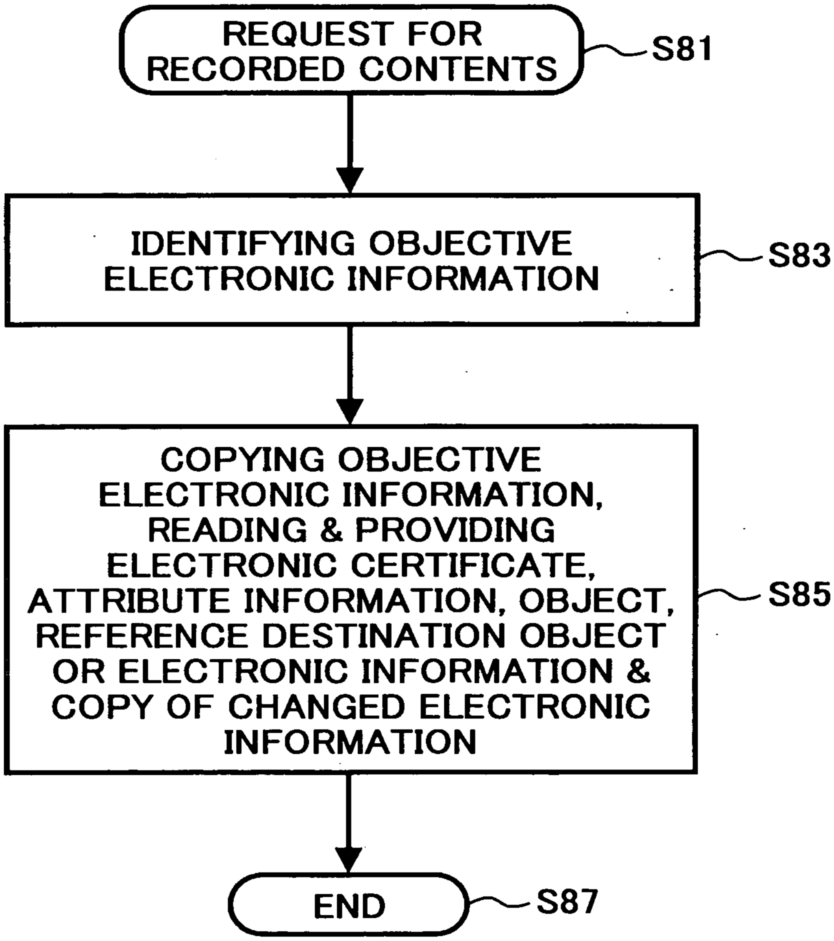

HTML DOCUMENT
OBJECT
ATTRIBUTE INFORMATION
HTML DOCUMENT (CHANGED)
HASH VALUE 1
REFERENCE DOCUMENT (OR OBJECT)
ATTRIBUTE INFORMATION
HASH VALUE 2

FIG. 13


REQUEST FOR RECORDED CONTENTS
S81
IDENTIFYING OBJECTIVE ELECTRONIC INFORMATION
S83
COPYING OBJECTIVE ELECTRONIC INFORMATION, READING & PROVIDING ELECTRONIC CERTIFICATE, ATTRIBUTE INFORMATION, OBJECT, REFERENCE DESTINATION OBJECT OR ELECTRONIC INFORMATION & COPY OF CHANGED ELECTRONIC INFORMATION
S85
END
S87